IT-21022

Q1. Let, 'p' be a prime number and 'a' be an integer that not divisible by p, then

$$a^{p-1} = 1 \pmod p$$

proof of Fermat's Little Theorem:-

Let 'a' be such that $\gcd(a,p) = 1$ and considers the set of integers:

$$S = \{1, 2, 3, \dots p-1\}$$

multiply each element in the set by a module p

$$aS = \{a, 2a, 3a, \dots, a(p-1)\} \bmod p$$

Since, $\gcd(a,p) = 1$, multiplying by a is a bijection in module p, so no two elements $a.i = a.j$ mod p for $i \neq j$

$$\prod_{i=1}^{p-1} i = \prod_{i=1}^{p-1} (a.i) \bmod p$$

$$\prod_{i=1}^{p-1} (a \cdot i) = a^{p-1} \prod_{i=1}^{p-1} i$$

$$\prod_{i=1}^{p-1} i \equiv a^{p-1} \prod_{i=1}^{p-1} i \pmod{p}$$

$$1 \equiv a^{p-1} \pmod{p}$$

Hence: Fermat's Little Theorem is proved

Example:

Given $a = 7$, $p = 13$

$\therefore \gcd(13, 7) = 1$ apply Fermat's little theorem.

$$7^{12} \equiv 1 \pmod{13}$$

So, $7^{12} \bmod 13 = 1$.

~~Apply~~

Application in RSA Cryptography:

RSA (Rivest-Shamir-Adleman) is a public Key-cryptosystem that relies heavily on on numbers theory and modular arithmetic

fermat's Little Theorem helps in:

(i) Reduces large powers modulo a prime during encryption and decryption.

Q2. Prime factorization of $n = 3545100$.

$\therefore 3545100 = 2^2 \times 3^3 \cdot 5^2 \cdot 13 \cdot 101$

Euler's Totient function formula:

if, $n = p_1^{k_1} \cdot p_2^{k_2}, \ldots p_m^{k_m}$

then, $\phi(n) = n \cdot \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right)$

So, $\phi(3545100) = 3545100 \cdot (1 - 1/2) \cdot (1 - 1/3) \cdot (1 - 1/5) \cdot (1 - 1/101)$

$= 3545100 \cdot \frac{1 \cdot 2 \cdot 4 \cdot 12 \cdot 100}{2 \cdot 3 \cdot 5 \cdot 13 \cdot 101}$

$\Rightarrow 1 \cdot 2 \cdot 4 \cdot 12 \cdot 100 = 9600$

$2 \cdot 3 \cdot 5 \cdot 13 \cdot 101 = 39390$

$\therefore \phi(3545100) \approx 864864$

(Ans.)

Q3. Given Congruences:

$x \equiv 2 \bmod 3$

$x \equiv 3 \bmod 4$

$x \equiv 1 \bmod 5$

Let, $m_1 = 3, m_2 = 4 ; m_3 = 5$

$N = 3 \cdot 4 \cdot 5 = 60$

$\therefore \ x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \bmod N$

where,

$a_1 = 2, a_2 = 3; a_3 = 1$

$M_i = \frac{N}{m_i}$

$y_i = M_i^{-1} \bmod m_i$

Compute M_i

$M_1 = \frac{60}{3\cancel{0}} = 20$

$M_2 = \frac{60}{4} = 15$

$M_3 = \frac{60}{5} = 12$

Now, Compute y_i

$20 \cdot y_1 \equiv 1 \bmod 3 \quad \Rightarrow y_1 = 2$

$15 \cdot y_2 \equiv 1 \bmod$

$y_2 = 3$

$12 \cdot y_3 \equiv 1 \bmod 5$

$\Rightarrow y_3 = 3$

$x \equiv 2 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 1 \cdot 12 \cdot 3 \quad \bmod 60$

$\equiv 80 + 135 + 36 = 251 \bmod 60$

$\therefore 251 \bmod 60 = 11$.

$\therefore \boxed{x \equiv 11 \bmod 60}$

(Ans.)

Q4. A Carmichael number is a composite number n such that for all integers a with $\gcd(a, n) = 1$ it satisfies.

$$a^{n-1} \equiv 1 \pmod{n}$$

prime factorization of 561

$$561 = 3 \times 11 \times 17$$

Now,

$3 - 1 = 2 \mid 560$

$11 - 1 = 10 \mid 560$

$17 - 1 = 16 \mid 560$

All three satisfy the condition.

So, 561 is a carmichale number.

Q5. A number g is a primitive root modulo 17

$$ord_{17}(g) = 16$$

That is $g^K \not\equiv 1 \mod 17$ for all $K<16$ but $g^{16} \equiv 1$

$$g^{\frac{16}{q}} \not\equiv 1 \mod 17 \text{ for all prime divisors}$$

we must check:

$g^8 \not\equiv 1 \mod 17$

$g^4 \not\equiv 1 \mod 17$

$g^2 \not\equiv 1 \mod 17$

Now, $g = 3$ (let)

$3^2 = 9 \mod 17 \neq 1$

$3^4 = 81 \mod 17 = 13 \neq 1$

$3^8 = 13^2 = 16 \mod 17 = 16 \neq 1$

Finally, $3^{16} \mod 17 = 1$.

So, $g = 3$ passes all the tests.

CamScanner

Q6. Let's Compute $3^x \bmod 17$ for $x = 1$ to 16.

x	$3^x \bmod 17$
1	3
2	9
3	10
4	13

we find $3^4 \equiv 13 \bmod 17$.

$\therefore x = 4$ (Ans.)

Q7. The discrete logarithm plays a centra role in the Diffie-Hellman Key Exchange protocol, which allows two parties to se-curely share a secret key over a publ channel.

The role of the Discrete Logarithm:

The security of Diffie-Hellman relies on the difficulty of the Discrete Logarithm

Given g, p and $A = g^a \bmod p$, find a

This is computationally hard for large primes, and there is no efficient algorithm known to solve it in general.

This makes it infesible for an eaves-droppers to determine the shared secre

Q8. Comparison among substitution cipher, Transposition cipher, playfair cipher. Given bellow.

Feature	Substitition Cipher	Transposition	playfair cipher
Mechanism	Replace letters	Rearrang letter	Replace letter pairs
Key space	Caesar	Depends on permutation	25!
Frequency	Preserved	Preserved	Disguised
Frequency Attack	Easy.	Medium	Harder
Example	HELLO → KHOOR	HELLO → LEHLO	HELLO → CFPP

IT-21022

Q9. a) Encrypt the plaintext "Dept of ICT, MB-STU"

plaintext: DEPTOFICTMBSTU.

Convert letters to numbers

Letter	pos	Apply $(5x+8) \bmod 26$	Cipher
D	3	$(5\times3+8) = 23$	X
E	4	$5\times4+8 = 28 \to 2$	C
P	15	$5\times15+8 = 83 \to 5$	F
T	19	$5\times 19+8 \to 78 \to 0$	A
⋮			
U	20	$5\times20+8 = 108 \to 4$	E

∴ So, the final Ciphertext:

XCFZAHWSZQNUZE

Q10. Encryption process:

step 1: Substitution (shift Based on PRNG)

(i) Generate a pseudo-random shift-value using a speed.

~~(ii)~~

step 2: permutation

(i) Group text into blocks of 4.

(ii) Apply fixed permutation pattern [3, 1, 4, 2]

Example: TESTC~~IPHER~~

Substitution:

$T(19) + 1 = U(20)$

$E(4) + 3 = H(7)$

$S(18) + 2 = U(20)$

$T(19) + 4 = X(23)$

→ "UHUX"

• Permutation [3, 1, 4, 2] → UHUX → UUXH

∴ Final ciphertext $\boxed{UUXH}$

(Ans.)